



The state of application security in 2024

The imperative of driving closer alignment among the CISO, CEO, and board

Dynatrace C-Suite Insights Report

What's inside

CHAPTER ONE

Security leaders need to replace technical jargon with precise messages about business risk

CHAPTER TWO

Application security is an Achilles' heel

CHAPTER THREE

SolarWinds and MOVEit incidents have given third-party risk management new urgency

CHAPTER FOUR

Automation across the DevSecOps lifecycle is central to risk management

CHAPTER FIVE

Traditional tools and practices have limited value in the cloud-native, AI-driven threat landscape

CONCLUSION

The unique value of Dynatrace

APPENDIX

Methodology and global data summary

Introduction

There is no doubt that cybersecurity has become a board-level issue. The impact of a data breach can range from regulatory fines to damaged consumer trust and brand reputation or even reduced market share. New regulations are also increasingly holding organizational leaders accountable for their ability to prepare and respond to security incidents. These factors have elevated cybersecurity to a C-suite and board-level concern.

However, executive engagement has often been limited to conversations around regulatory compliance and high-profile or user-centric security risks, such as phishing attacks, ransomware, or the use of mobile devices among an increasingly hybrid workforce. There is often less understanding of the material operational effects created by other, more technology-centric risks, such as gaps in the organization's application security posture.

This report examines the challenges that chief information security officers (CISOs) face in increasing their organization's understanding of these issues. It highlights how a unified observability and security strategy can help them engage the wider C suite to improve their organization's risk posture.



VOICE OF THE CEO

“Our investors remain concerned about the financial risks associated with cyberattacks. [Being a company that holds customers' data,] another primary concern is...that their information and back-end data are safe and secure.”

— CEO, U.S. software and technology company

CHAPTER ONE

Security leaders need to replace technical jargon with precise messages about business risk

In a digital-first world, organizations are constantly combatting adversaries seeking to exploit vulnerabilities that enable them to access sensitive data. As C-suite executives have become more aware of this risk, CISOs face a growing need to report cyberthreats to them, establishing a culture of shared responsibility for security management. However, a significant proportion of organizations still need to go further to bring the topic of security into the boardroom.

Organizations that regularly require CISOs to report to the CEO and board on their cybersecurity risk and compliance posture

65% Yes

35% No

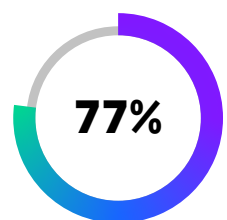


VOICE OF THE CEO

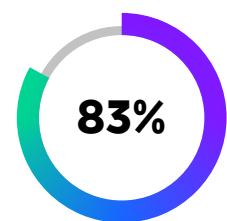
“In the cyberattack world, it's not about pointing fingers at one person and blaming them. In our organization, we see it as a shared responsibility. Even with all the policies and tools in place, there's still a chance that an attack could happen. We understand there's no fool-proof protection against cyberthreats.”

– CEO, U.S. retail company

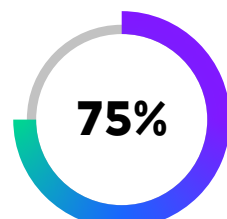
Despite their growing interest and engagement in their organization's cybersecurity posture, C-suite executives have a limited understanding of the risk landscape and different priorities that drive security decisions. As a result, they don't always see eye-to-eye with CISOs and the IT department. CISOs urgently need to drive greater alignment between security teams and the board by elevating the discussion around cybersecurity from bits and bytes to business risk.



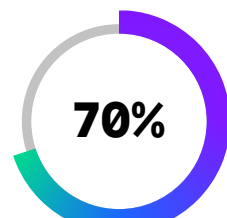
of CISOs say boards and CEOs focus too heavily on the ability to react to security incidents and not enough on reducing and preventing risk proactively.



of CISOs say their board of directors and CEO need to understand their security posture better so they can assess business risk and compliance requirements.



of CISOs say their security tools have limited ability to generate insights the CEO and board can use to understand business risk and prevent threats.



of C-suite executives say security teams often talk in technical terms without providing business context and believe the CISO is responsible for bridging the gap.

VOICE OF THE CFO


“Explaining the problems or threats our security team has analyzed to other stakeholders or C-suite executives who are not directly involved with security technology is always a concern.”

– CFO, U.K. education provider

Application security is an Achilles' heel


Applications remain one of the most common initial access vectors for cyberattacks. In fact, nearly three-quarters of organizations have experienced a security incident related to one of their applications in the past two years. This has driven application security to the top of the risk management agenda for IT departments and business leaders alike.

CISOs ranked their organizations' top priorities for cybersecurity management as the following:*




1. Application security

(i.e., vulnerability management)



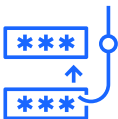
2. Crisis management and response

(i.e., data breach and media focus)




3. Internal risk management or oversight

(i.e., use of mobile devices)




4. Human error or insider threats

(i.e., phishing or corporate espionage)




5. Third-party risk management

(i.e., cloud services or supply chain)



6. Disruption to operations

(i.e., denial of service or system downtime)



7. Regulatory compliance

(i.e., HIPAA and PCI DSS)

*Based on the percentage of respondents that ranked each category as priority 1, 2, or 3

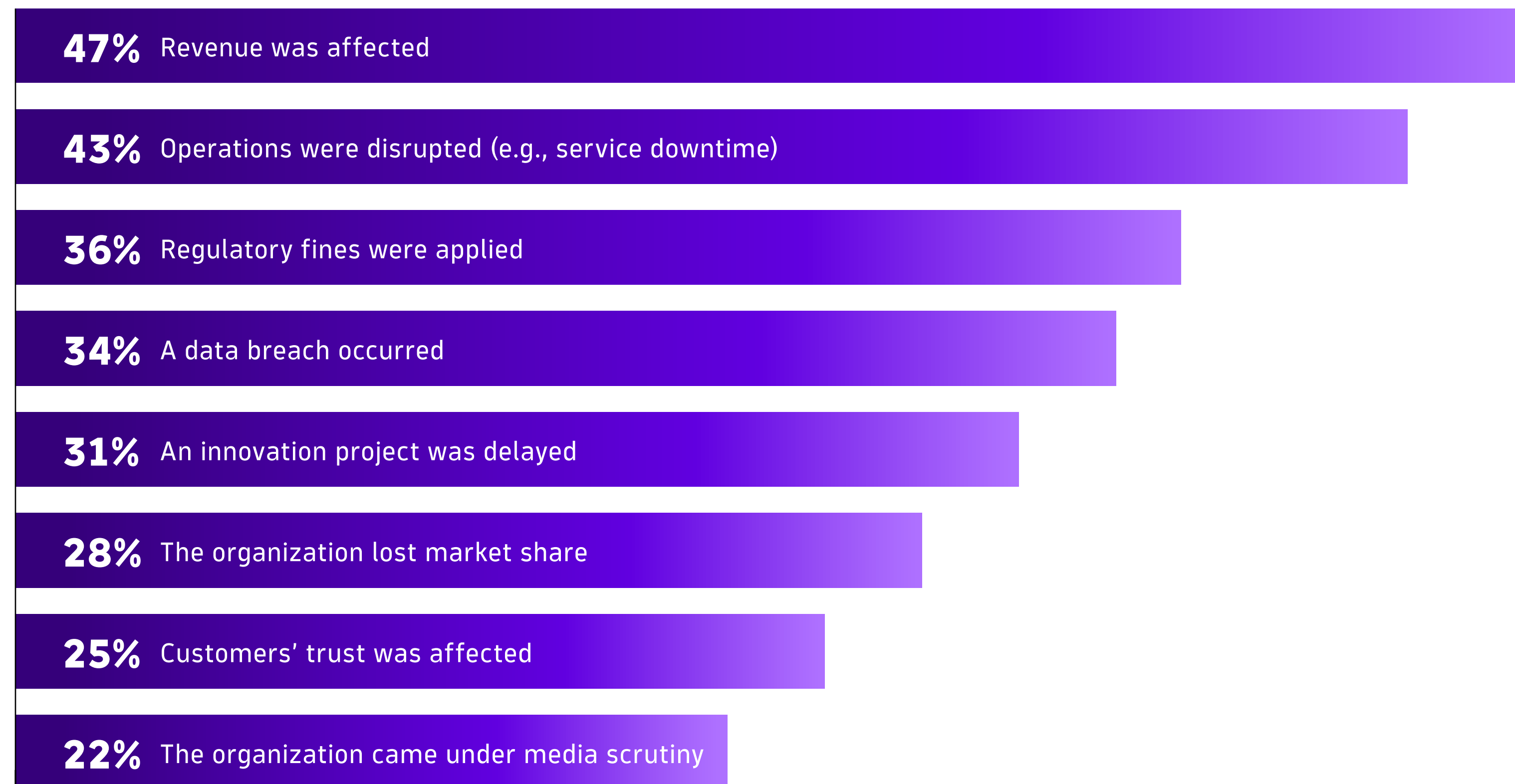
VOICE OF THE CEO

“Every industry has stringent regulations about keeping data safe. Application security is essential for meeting these rules — GDPR and DSS. If we don’t do an excellent job securing our applications, it could mean significant fines, a damaged reputation, and even legal trouble.”

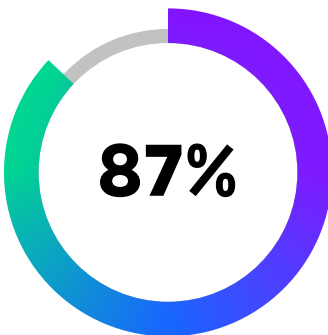
– CEO, U.S. retail company

72% of organizations have experienced an application security incident in the past two years.

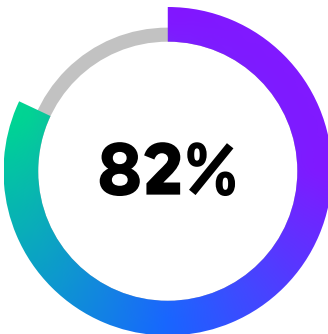
The most common costs and effects of these application security incidents include the following:



CISOs have yet to identify a consistent approach to providing the board with clear insight into their organization's application security risk posture. This leaves executives blind to the potential effect of vulnerabilities and makes it difficult to make informed decisions to protect the organization from operational, financial, and reputational damage.



of CISOs say application security is a blind spot at the CEO and board level.



of CISOs say they urgently need to increase the visibility of their CEO and board into application security risk to enable more informed decisions to strengthen defenses.

Security teams report the following key metrics or insights to the board and CEO to inform them of application security risk:

47%

A precise risk score is attributed to any new vulnerability as it emerges, based on the impact on our business

45%

Severity score for critical vulnerabilities — e.g., the Common Vulnerability Scoring System (CVSS)

42%

Forecasted cost or business impact of an exploited vulnerability

38%

Number and type of vulnerabilities in any period

35%

Time to remediate critical security vulnerabilities

32%

Number of critical vulnerabilities currently live

CHAPTER THREE

SolarWinds and MOVEit have given third-party risk management new urgency

Organizations rely heavily on software from external providers, which exposes them to additional risk. Following the widespread impact and response to the SolarWinds and MOVEit security incidents, organizations are urgently reevaluating their approaches to third-party risk management to better manage the integrity of their software supply chain.

Every organization has altered its approach to third-party risk management in the wake of the SolarWinds and MOVEit incidents. The most common changes include the following:

58%
Implementing third-party risk management (TPRM) practices, defining clear security requirements and contracts with vendors

47%
Continually monitoring and auditing vendors' compliance with security standards like SOC 2 or ISO 27001

51%
Reviewing vendors' software bill of materials (SBOM) to understand the components and dependencies within software to identify potential risks

43%
Scrutinizing the way vendors build and test software and ensure they maintain secure coding and patching practices

VOICE OF THE CEO

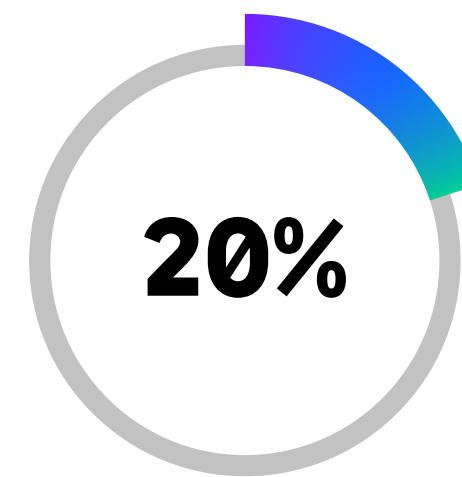
"We heavily rely on our information technology systems and those of our vendors across our business operations. However, they are susceptible to various risks and potential disruptions.

To mitigate such risks and ensure the continued reliability of our information systems, we maintain rigorous security measures, conduct regular maintenance and updates, and implement redundancy and backup protocols."

— CEO, U.S. retail and wholesale company



of CISOs have not yet brought third-party software bills of materials (SBOMs) into their organization's risk management practices.



of CISOs say third-party SBOMs regularly provide insights that improve risk management.

It's not enough to simply know whether a third-party vulnerability exists within an organization's environment. Security teams also need to quickly and conclusively determine the extent of exposure and the risk it poses to the business, identify whether it has been exploited — and if so, to what effect — and then share that insight with executive leaders.

VOICE OF THE CFO

"The CISO connects the bridge between what is going on in the IT and cybersecurity departments and the business. They provide real-time insights into the factors of application security that might impact the industry.

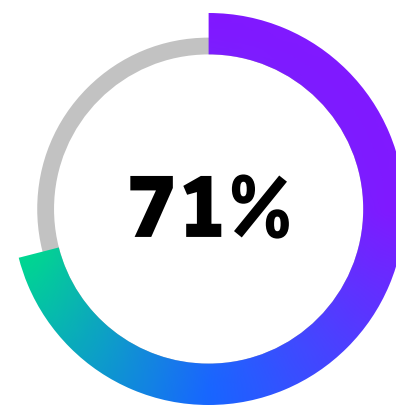
For example, in a board meeting, the CISO translates technical vulnerabilities into an analysis of the probable business risks they might cause."

— CFO, U.K. education provider

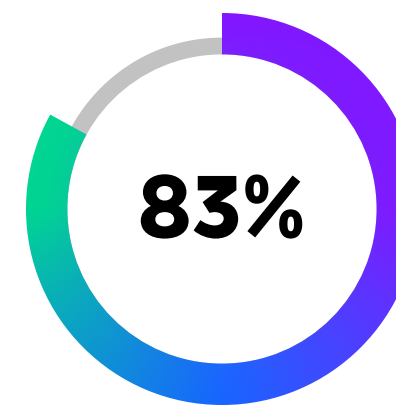
CHAPTER FOUR

Automation across the DevSecOps lifecycle is central to risk management

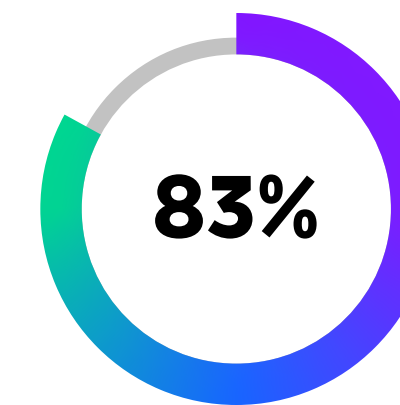
As digital innovation accelerates, organizations are increasingly looking to automate processes across the DevOps and security (DevSecOps) lifecycle to minimize risk and maintain regulatory compliance. This practice will become even more critical as cybercriminals continue to use AI to create new exploits faster and leverage them at scale while development teams use those capabilities to speed up software delivery with less manual oversight.



71% of CISOs say DevSecOps automation is critical to ensuring reasonable measures have been taken to minimize application security risk.



83% of CISOs say DevSecOps automation will be essential to their ability to stay on top of emerging regulations such as the Securities and Exchange Commission (SEC) cybersecurity mandate, the Network and Information Security Directive (NIS2), and the Digital Operational Resilience Act (DORA).



83% of CISOs say DevSecOps automation is even more important to managing the risk of vulnerabilities introduced by using AI.

Mature DevSecOps automation practices are essential to organizations' ability to accelerate innovation. This capability helps teams to drive consistency in development and security processes while reducing the risk of human error allowing vulnerabilities to enter production in the first place. However, most organizations are in the early stages of DevSecOps automation, as teams continue to rely on siloed practices.

75%

of CISOs say they urgently need to improve the maturity of DevSecOps automation.

54%

of CISOs say their DevSecOps automation practices are absent or emerging.

11%

of CISOs say their organization has mature DevSecOps automation practices.

70%

of CISOs say the need for multiple application security tools drives operational inefficiency due to the effort needed to make sense of disparate sources of data.

VOICE OF THE CFO

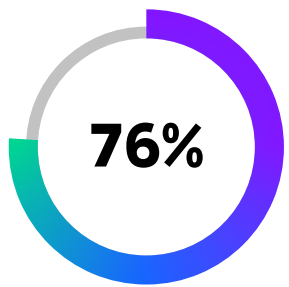
“[We] continue to invest in our people to make sure that they’re skilled to respond to incidents. We’re also starting to look at more tools that automate the process and help us with managing incidents so we’re more efficient and effective in the processes of how we respond if something goes wrong.”

– CFO, Australian financial services company

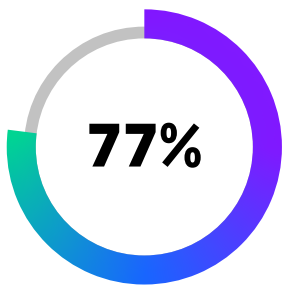
CHAPTER FIVE

Traditional tools and practices have limited value in the cloud-native, AI-driven threat landscape

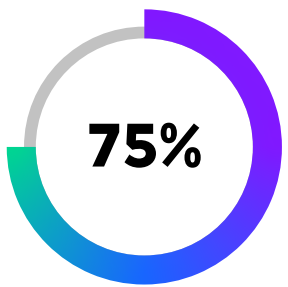
The growing complexity of cloud-native architectures is rendering traditional security tools and practices obsolete. Log-based security information and event management (SIEM) and extended detection and response (XDR) solutions may have served teams well in the past, but they are unable to keep up with the distributed and dynamic nature of cloud-native architectures and multicloud environments. As a result, security teams are unable to surface the data-driven insights that the CEO and board-level executives need to understand their organization’s risk posture.



of CISOs cite the limitations of security tools for real-time identification of risks in dynamic cloud-native architectures as a key challenge.



of CISOs say current tools such as XDR and SIEM are unable to manage cloud complexity, as they lack the intelligence needed to drive automation at scale.



of CISOs cite the prevalence of blind spots due to the limitations or restrictions upon agent-based security tooling as a key challenge.

VOICE OF THE CFO

“When security teams talk to different teams, they should relate to the goals they’re trying to achieve rather than talking about the technical terms of attacks or different types of threats or technology solutions we have. It’s about keeping it basic and using business language so people can relate.”

– CFO, Australian financial services company

The increased use of AI within organizations and by those seeking to breach their defenses creates a further concern. While AI tools can help developers accelerate innovation, they also equip cybercriminals with the means to quickly create and leverage new exploits. As a result, organizations need to modernize their security practices to enable them to keep up with a more dynamic and unpredictable threat landscape.

CISOs' top concerns relating to the risk of increased AI use in their organizations include the following:

- 52%** Risk of cybercriminals using AI to create new vulnerability exploits faster and execute them on a wider scale
- 47%** Risk of AI resulting in inappropriate data use, leading to noncompliance
- 45%** Risk of AI being used to accelerate software development, with less oversight leading to more security vulnerabilities

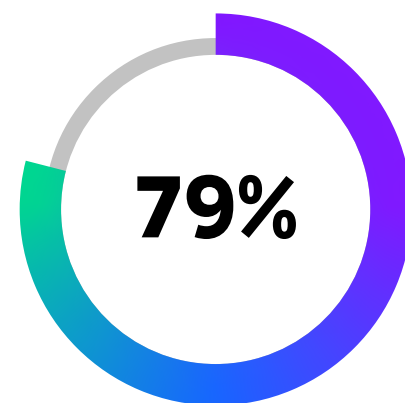
VOICE OF THE CEO

“The risk of AI is anticipated to proliferate as [these technologies] become inexpensive and more available. For example, you can fake ChatGPT into scripting a code or a message from anybody requesting assistance.

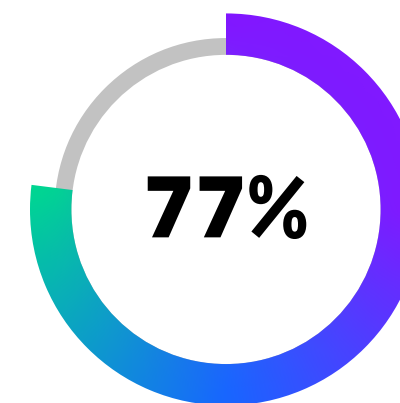
There is also increasing confidentiality apprehensiveness as more clients raise the issue of efficiently distributing restricted data with AI.”

— CEO, Australian telecommunications company

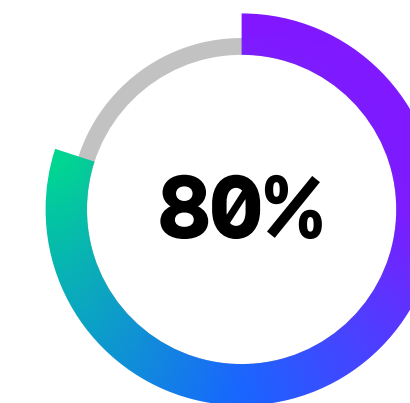
The use of multiple tools and the reliance on siloed processes also drive inefficiencies. These factors make it difficult for teams to maintain the end-to-end visibility needed to identify the risk of vulnerabilities and ensure that exposures are prioritized and dealt with quickly. To protect their applications and data from modern, advanced cyber threats, organizations need a unified approach to security supported by a platform that drives mature DevSecOps automation and harnesses AI to deal with distributed data at any scale.



of CISOs say vulnerability management and threat detection, investigation, and response can no longer be siloed processes.



of CISOs say current tools such as XDR and SIEM lose effectiveness due to silos across threat detection, investigation, and response processes.



of CISOs say their investments in SIEM and XDR tools would be better shifted into solutions that enable intelligent threat detection and response for business-critical cloud applications based on real-time attack insights.

CONCLUSION

The unique value of Dynatrace

Optimized for cloud-native applications, containers, and Kubernetes, Dynatrace® Application Security, as part of the Dynatrace® platform, automatically and continuously detects vulnerabilities in applications at runtime. It also provides real-time detection and blocking to protect against injection attacks that exploit critical vulnerabilities. By unifying observability and security data, it removes blind spots, helps to ensure development teams aren't wasting time chasing false positives, and provides the C suite with confidence in the security of their organizations' applications.

Dynatrace Application Security enables CISOs and their teams to:



Drive a unified observability and security strategy that helps CISOs to engage wider C-suite executives, supporting their effort to improve their organization's overall risk posture.



Identify and remediate exposure risk 95% faster with runtime vulnerability analysis. Know within minutes when a critical application vulnerability is introduced to production. Confidently implement countermeasures and remediate with automated analysis of runtime context and security intelligence.



Focus on what matters with Davis® AI-assisted prioritization. Teams receive the precise information they need to resolve the most critical vulnerabilities first. Davis AI uses security intelligence and runtime context to determine risk based on criteria such as internet exposure.



Continuously identify exposures with runtime application protection. Detect and block common attacks on application-layer vulnerabilities, such as injection attacks. Protect against critical zero-day attack types while the vulnerability is being remediated.



Get fast insights by analyzing observability and security data. Reduce the cost of investigating alerts from multiple tools to immediately understand the impact of a security incident, such as a critical application vulnerability. Quickly verify what happened, leverage observability context to analyze the risk or impact, and access actionable insights needed to respond effectively.

Methodology and global data summary

This report is based on a global survey of 1,300 CISOs in large enterprises with over 1,000 employees. It was commissioned by Dynatrace and conducted by Coleman Parkes between March and April 2024.

The sample included 200 respondents in the U.S.; 150 in the Middle East; 100 each in the U.K., France, Germany, Italy, Spain, Australia, and Japan; and 50 each in Sweden, Benelux, India, Brazil, and Mexico.

It also includes insights from 10 in-depth interviews that Coleman Parkes conducted with CEOs and CFOs across the U.S., U.K., and Australia in March 2024.

U.S.

Sample base: 200 respondents

- **59%** of CISOs say there is a regular requirement to report to the CEO and board on their cybersecurity risk and compliance posture.
- **74%** of CISOs say their security tools have limited ability to generate insights the CEO and board can use to understand business risk and prevent threats.
- CISOs ranked their organizations' top priorities for cybersecurity management as the following:*
 - 1** — Application security (i.e., vulnerability management)
 - 2** — Crisis management and response (i.e., data breach and media focus)
 - 3** — Human error / insider threats (i.e., phishing or corporate espionage)
- **66%** of organizations have experienced an application security incident in the past two years.
- **86%** of CISOs say application security is a blind spot at the CEO and board level.
- **84%** of CISOs say DevSecOps automation will be essential to their ability to stay on top of emerging regulations such as the SEC cybersecurity mandate, NIS2, and DORA.
- **83%** of CISOs say DevSecOps automation is even more important to managing the risk of vulnerabilities introduced by AI.
- **77%** of CISOs have difficulty driving DevSecOps automation due to their reliance on multiple application security tools.
- Only **13%** of CISOs say their organization has mature DevSecOps automation practices.

Brazil

Sample base: 50 respondents

- **64%** of CISOs say there is a regular requirement to report to the CEO and board on their cybersecurity risk and compliance posture.
- **80%** of CISOs say their security tools have limited ability to generate insights the CEO and board can use to understand business risk and prevent threats.
- CISOs ranked their organizations' top priorities for cybersecurity management as the following:*
 - 1** — Crisis management and response (i.e., data breach and media focus)
 - 2** — Application security (i.e., vulnerability management)
 - 3** — Internal risk management / oversight (i.e., use of mobile devices)
 - Third-party risk management (i.e., cloud services or supply chain)
 - Regulatory compliance (i.e., HIPAA and PCI DSS)
- **84%** of organizations have experienced an application security incident in the past two years.
- **90%** of CISOs say application security is a blind spot at the CEO and board level.
- **82%** of CISOs say DevSecOps automation will be essential to their ability to stay on top of emerging regulations such as the SEC cybersecurity mandate, NIS2, and DORA.
- **92%** of CISOs say DevSecOps automation is even more important to managing the risk of vulnerabilities introduced by AI.
- **80%** of CISOs have difficulty driving DevSecOps automation due to their reliance on multiple application security tools.
- Only **10%** of CISOs say their organization has mature DevSecOps automation practices.

Mexico

Sample base: 50 respondents

- **50%** of CISOs say there is a regular requirement to report to the CEO and board on their cybersecurity risk and compliance posture.
- **66%** of CISOs say their security tools have limited ability to generate insights the CEO and board can use to understand business risk and prevent threats.
- CISOs ranked their organizations’ top priorities for cybersecurity management as the following:*
- 1** — Application security (i.e., vulnerability management)
- 2** — Crisis management and response (i.e., data breach and media focus)
- 3** — Internal risk management / oversight (i.e., use of mobile devices)
- **50%** of organizations have experienced an application security incident in the past two years.
- **90%** of CISOs say application security is a blind spot at the CEO and board level.
- **78%** of CISOs say DevSecOps automation will be essential to their ability to stay on top of emerging regulations such as the SEC cybersecurity mandate, NIS2, and DORA.
- **92%** of CISOs say DevSecOps automation is even more important to managing the risk of vulnerabilities introduced by AI.
- **64%** of CISOs have difficulty driving DevSecOps automation due to their reliance on multiple application security tools.
- Only **16%** of CISOs say their organization has mature DevSecOps automation practices.

U.K.

Sample base: 100 respondents

- **69%** of CISOs say there is a regular requirement to report to the CEO and board on their cybersecurity risk and compliance posture.
- **75%** of CISOs say their security tools have limited ability to generate insights the CEO and board can use to understand business risk and prevent threats.
- CISOs ranked their organizations’ top priorities for cybersecurity management as the following:*
- 1** — Internal risk management / oversight (i.e., use of mobile devices)
- 2** — Crisis management and response (i.e., data breach and media focus)
- 3** — Human error / insider threats (i.e., phishing or corporate espionage)
- **65%** of organizations have experienced an application security incident in the past two years.
- **90%** of CISOs say application security is a blind spot at the CEO and board level.
- **84%** of CISOs say DevSecOps automation will be essential to their ability to stay on top of emerging regulations such as the SEC cybersecurity mandate, NIS2, and DORA.
- **79%** of CISOs say DevSecOps automation is even more important to managing the risk of vulnerabilities introduced by AI.
- **82%** of CISOs have difficulty driving DevSecOps automation due to their reliance on multiple application security tools.
- Only **8%** of CISOs say their organization has mature DevSecOps automation practices.

France

Sample base: 100 respondents

- **68%** of CISOs say there is a regular requirement to report to the CEO and board on their cybersecurity risk and compliance posture.
- **72%** of CISOs say their security tools have limited ability to generate insights the CEO and board can use to understand business risk and prevent threats.
- CISOs ranked their organizations’ top priorities for cybersecurity management as the following:*
- 1** — Application security (i.e., vulnerability management)
- 2** — Crisis management and response (i.e., data breach and media focus)
- 3** — Internal risk management / oversight (i.e., use of mobile devices)
- **74%** of organizations have experienced an application security incident in the past two years.
- **81%** of CISOs say application security is a blind spot at the CEO and board level.
- **89%** of CISOs say DevSecOps automation will be essential to their ability to stay on top of emerging regulations such as the SEC cybersecurity mandate, NIS2, and DORA.
- **77%** of CISOs say DevSecOps automation is even more important to managing the risk of vulnerabilities introduced by AI.
- **73%** of CISOs have difficulty driving DevSecOps automation due to their reliance on multiple application security tools.
- Only **11%** of CISOs say their organization has mature DevSecOps automation practices.

Germany

Sample base: 100 respondents

- **71%** of CISOs say there is a regular requirement to report to the CEO and board on their cybersecurity risk and compliance posture.
- **76%** of CISOs say their security tools have limited ability to generate insights the CEO and board can use to understand business risk and prevent threats.
- CISOs ranked their organizations’ top priorities for cybersecurity management as the following:*
- 1** — Internal risk management / oversight (i.e., use of mobile devices)
- 2** — Application security (i.e., vulnerability management)
- 3** — Disruption to operations (i.e., denial of service or systems downtime)
- **79%** of organizations have experienced an application security incident in the past two years.
- **90%** of CISOs say application security is a blind spot at the CEO and board level.
- **84%** of CISOs say DevSecOps automation will be essential to their ability to stay on top of emerging regulations such as the SEC cybersecurity mandate, NIS2, and DORA.
- **93%** of CISOs say DevSecOps automation is even more important to managing the risk of vulnerabilities introduced by AI.
- **83%** of CISOs have difficulty driving DevSecOps automation due to their reliance on multiple application security tools.
- Only **9%** of CISOs say their organization has mature DevSecOps automation practices.

Italy

Sample base: 100 respondents

- **64%** of CISOs say there is a regular requirement to report to the CEO and board on their cybersecurity risk and compliance posture.
- **71%** of CISOs say their security tools have limited ability to generate insights the CEO and board can use to understand business risk and prevent threats.
- CISOs ranked their organizations' top priorities for cybersecurity management as the following:*)
 - 1** — Application security (i.e., vulnerability management)
 - 2** — Crisis management and response (i.e., data breach and media focus)
 - 3** — Internal risk management / oversight (i.e., use of mobile devices)
 - Disruption to operations (i.e., denial of service or systems downtime)
- **72%** of organizations have experienced an application security incident in the past two years.
- **91%** of CISOs say application security is a blind spot at the CEO and board level.
- **82%** of CISOs say DevSecOps automation will be essential to their ability to stay on top of emerging regulations such as the SEC cybersecurity mandate, NIS2, and DORA.
- **83%** of CISOs say DevSecOps automation is even more important to managing the risk of vulnerabilities introduced by AI.
- **82%** of CISOs have difficulty driving DevSecOps automation due to their reliance on multiple application security tools.
- Only **10%** of CISOs say their organization has mature DevSecOps automation practices.

Spain

Sample base: 100 respondents

- **68%** of CISOs say there is a regular requirement to report to the CEO and board on their cybersecurity risk and compliance posture.
- **73%** of CISOs say their security tools have limited ability to generate insights the CEO and board can use to understand business risk and prevent threats.
- CISOs ranked their organizations' top priorities for cybersecurity management as the following:*)
 - 1** — Internal risk management / oversight (i.e., use of mobile devices)
 - 2** — Third-party risk management (i.e., cloud services or supply chain)
 - 3** — Crisis management and response (i.e., data breach and media focus)
- **76%** of organizations have experienced an application security incident in the past two years.
- **86%** of CISOs say application security is a blind spot at the CEO and board level.
- **78%** of CISOs say DevSecOps automation will be essential to their ability to stay on top of emerging regulations such as the SEC cybersecurity mandate, NIS2, and DORA.
- **82%** of CISOs say DevSecOps automation is even more important to managing the risk of vulnerabilities introduced by AI.
- **76%** of CISOs have difficulty driving DevSecOps automation due to their reliance on multiple application security tools.
- Only **17%** of CISOs say their organization has mature DevSecOps automation practices.

Sweden

Sample base: 50 respondents

- **58%** of CISOs say there is a regular requirement to report to the CEO and board on their cybersecurity risk and compliance posture.
- **68%** of CISOs say their security tools have limited ability to generate insights the CEO and board can use to understand business risk and prevent threats.
- CISOs ranked their organizations' top priorities for cybersecurity management as the following:*
- **1** — Internal risk management / oversight (i.e., use of mobile devices)
- **2** — Third-party risk management (i.e., cloud services or supply chain)
- **3** — Human error / insider threats (i.e., phishing or corporate espionage)
- Crisis management and response (i.e., data breach and media focus)
- **72%** of organizations have experienced an application security incident in the past two years.
- **84%** of CISOs say application security is a blind spot at the CEO and board level.
- **82%** of CISOs say DevSecOps automation will be essential to their ability to stay on top of emerging regulations such as the SEC cybersecurity mandate, NIS2, and DORA.
- **78%** of CISOs say DevSecOps automation is even more important to managing the risk of vulnerabilities introduced by AI.
- **64%** of CISOs have difficulty driving DevSecOps automation due to their reliance on multiple application security tools.
- Only **12%** of CISOs say their organization has mature DevSecOps automation practices.

Benelux

Sample base: 50 respondents (32 Netherlands, 10 Belgium, 8 Luxembourg)

- **62%** of CISOs say there is a regular requirement to report to the CEO and board on their cybersecurity risk and compliance posture.
- **82%** of CISOs say their security tools have limited ability to generate insights the CEO and board can use to understand business risk and prevent threats.
- CISOs ranked their organizations' top priorities for cybersecurity management as the following:*
- **1** — Crisis management and response (i.e., data breach and media focus)
- **2** — Human error / insider threats (i.e., phishing or corporate espionage)
- **3** — Third-party risk management (i.e., cloud services or supply chain)
- **76%** of organizations have experienced an application security incident in the past two years.
- **82%** of CISOs say application security is a blind spot at the CEO and board level.
- **84%** of CISOs say DevSecOps automation will be essential to their ability to stay on top of emerging regulations such as the SEC cybersecurity mandate, NIS2, and DORA.
- **72%** of CISOs say DevSecOps automation is even more important to managing the risk of vulnerabilities introduced by AI.
- **72%** of CISOs have difficulty driving DevSecOps automation due to their reliance on multiple application security tools.
- Only **2%** of CISOs say their organization has mature DevSecOps automation practices.

Middle East

Sample base: 150 respondents (65 UAE, 46 Saudi Arabia, 20 Kuwait, 19 Qatar)

- **73%** of CISOs say there is a regular requirement to report to the CEO and board on their cybersecurity risk and compliance posture.
- **77%** of CISOs say their security tools have limited ability to generate insights the CEO and board can use to understand business risk and prevent threats.
- CISOs ranked their organizations’ top priorities for cybersecurity management as the following: *
 - 1** — Internal risk management / oversight (i.e., use of mobile devices)
 - 2** — Third-party risk management (i.e., cloud services or supply chain)
 - 3** — Human error / insider threats (i.e., phishing or corporate espionage)
 - Crisis management and response (i.e., data breach and media focus)
- **76%** of organizations have experienced an application security incident in the past two years.
- **87%** of CISOs say application security is a blind spot at the CEO and board level.
- **80%** of CISOs say DevSecOps automation will be essential to their ability to stay on top of emerging regulations such as the SEC cybersecurity mandate, NIS2, and DORA.
- **81%** of CISOs say DevSecOps automation is even more important to managing the risk of vulnerabilities introduced by AI.
- **79%** of CISOs have difficulty driving DevSecOps automation due to their reliance on multiple application security tools.
- Only **10%** of CISOs say their organization has mature DevSecOps automation practices.

Australia

Sample base: 100 respondents

- **64%** of CISOs say there is a regular requirement to report to the CEO and board on their cybersecurity risk and compliance posture.
- **76%** of CISOs say their security tools have limited ability to generate insights the CEO and board can use to understand business risk and prevent threats.
- CISOs ranked their organizations’ top priorities for cybersecurity management as the following: *
 - 1** — Application security (i.e., vulnerability management)
 - 2** — Third-party risk management (i.e., cloud services or supply chain)
 - 3** — Disruption to operations (i.e., denial of service or systems downtime)
- **72%** of organizations have experienced an application security incident in the past two years.
- **89%** of CISOs say application security is a blind spot at the CEO and board level.
- **87%** of CISOs say DevSecOps automation will be essential to their ability to stay on top of emerging regulations such as the SEC cybersecurity mandate, NIS2, and DORA.
- **85%** of CISOs say DevSecOps automation is even more important to managing the risk of vulnerabilities introduced by AI.
- **80%** of CISOs have difficulty driving DevSecOps automation due to their reliance on multiple application security tools.
- Only **8%** of CISOs say their organization has mature DevSecOps automation practices.

Japan

Sample base: 100 respondents

- **64%** of CISOs say there is a regular requirement to report to the CEO and board on their cybersecurity risk and compliance posture.
- **76%** of CISOs say their security tools have limited ability to generate insights the CEO and board can use to understand business risk and prevent threats.
- CISOs ranked their organizations' top priorities for cybersecurity management as the following:*
- **1** — Application security (i.e., vulnerability management)
- **2** — Crisis management and response (i.e., data breach and media focus)
- **3** — Internal risk management / oversight (i.e., use of mobile devices)
- **73%** of organizations have experienced an application security incident in the past two years.
- **88%** of CISOs say application security is a blind spot at the CEO and board level.
- **77%** of CISOs say DevSecOps automation will be essential to their ability to stay on top of emerging regulations such as the SEC cybersecurity mandate, NIS2, and DORA.
- **84%** of CISOs say DevSecOps automation is even more important to managing the risk of vulnerabilities introduced by AI.
- **78%** of CISOs have difficulty driving DevSecOps automation due to their reliance on multiple application security tools.
- Only **15%** of CISOs say their organization has mature DevSecOps automation practices.

India

Sample base: 50 respondents

- **58%** of CISOs say there is a regular requirement to report to the CEO and board on their cybersecurity risk and compliance posture.
- **76%** of CISOs say their security tools have limited ability to generate insights the CEO and board can use to understand business risk and prevent threats.
- CISOs ranked their organizations' top priorities for cybersecurity management as the following:*
- **1** — Disruption to operations (i.e., denial of service or systems downtime)
- **2** — Application security (i.e., vulnerability management)
- **3** — Crisis management and response (i.e., data breach and media focus)
- Internal risk management / oversight (i.e., use of mobile devices)
- **70%** of organizations have experienced an application security incident in the past two years.
- **82%** of CISOs say application security is a blind spot at the CEO and board level.
- **90%** of CISOs say DevSecOps automation will be essential to their ability to stay on top of emerging regulations such as the SEC cybersecurity mandate, NIS2, and DORA.
- **76%** of CISOs say DevSecOps automation is even more important to managing the risk of vulnerabilities introduced by AI.
- **84%** of CISOs have difficulty driving DevSecOps automation due to their reliance on multiple application security tools.
- Only **4%** of CISOs say their organization has mature DevSecOps automation practices.

Automatic and intelligent observability for hybrid multiclouds

We hope this ebook has inspired you to take the next step in your digital journey. Dynatrace is committed to providing enterprises the data and intelligence they need to be successful with their enterprise cloud and digital transformation initiatives, no matter how complex.

Learn more

If you are ready to learn more, please visit www.dynatrace.com/platform for assets, resources, and a **free 15-day trial**.



[Dynatrace](#) (NYSE: DT) exists to make the world's software work perfectly. Our unified platform combines broad and deep observability and continuous runtime application security with the most advanced AIOps to provide answers and intelligent automation from data at enormous scale. This enables innovators to modernize and automate cloud operations, deliver software faster and more securely, and ensure flawless digital experiences. That's why the world's largest organizations trust the Dynatrace® platform to accelerate digital transformation.

Curious to see how you can simplify your cloud and maximize the impact of your digital teams? Let us show you. Sign up for a [free 15-day Dynatrace trial](#).

 **blog**  **@dynatrace**